

ОБҐРУНТУВАННЯ ВИБОРУ БІОМЕТРИЧНИХ СИСТЕМ ІДЕНТИФІКАЦІЇ

О. А. Баліцький^{1, а}, О. Д. Василенко¹

¹ Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
Фізико-технічний інститут

Анотація

Сьогодні більша частина систем біометричної ідентифікації використовується тільки з точки зору одного критерію – ризику першого та другого роду. При цьому безпечності використання такої системи для багатьох людей приділяється мінімальна увага. У доступній науково-технічній літературі практично відсутні кількісні характеристики різних відомих засобів стосовно зручності, безпечності та їх надійності. Нижче наведена спроба визначити різні чинники вибору того чи іншого засобу біометричної ідентифікації з огляду урахування вищезазначених характеристик.

Ключові слова: біометрична ідентифікація, доцільність використання, біометричні системи, сканування, відбитки пальців

Вступ

Незважаючи на те, що біометричні системи досить широко використовуються, все ж існують певні обмеження на поле їхнього застосування. Задля встановлення того, які саме обмеження та у яких системах вони присутні, необхідно дослідити кожну з запропонованих систем. Оцінка буде проводитись серед систем ідентифікації:

- 1) за відбитками пальців [1];
- 2) за райдужною оболонкою ока [2];
- 3) за комп'ютерним почерком [3];
- 4) за особливостями та характеристиками мовлення [4].

Доцільно встановити критерії оцінювання, які будуть базуватись на тому, де яка система може використовуватись і які можуть виникати незручності та шкідливі для здоров'я наслідки від користування ними.

1. Постановка задачі

Розглядатимемо системи з точки зору їх зручності, біологічної безпеки (тобто імовірності зараження після взаємодії системи з хворим користувачем) та часу їхнього напрацювання за різних умов експлуатації.

Дуже часто люди, мають різні захворювання, які можуть передаватися різними шляхами. Тому необхідно розглянути системи з урахуванням можливості передачі хвороби наступному користувачеві. В той же час важливими є надійність роботи, мобільність та зручність системи.

Для подальшого аналізу вважатимемо, що біометричні системи мають в першому наближенні практично однакові критерії ризику першого та другого

роду, що дасть змогу проводити їх оцінку акцентуючи увагу на дослідженні параметрів.

Будемо вважати, що кожен з вищезазначених показників має коефіцієнт за яким можливо оцінити його придатність до застосування. Тоді можна прийняти, що загальний коефіцієнт доцільності використання (K_{DB}) буде визначатись як добуток коефіцієнтів зручності (K_3), біологічної безпеки (K_{66}) та надійності (K_H) для оцінки систем. Значення кожного з цих коефіцієнтів (K_{DB} , K_3 , K_{66} , K_H) коливаються від 0 до 1, при цьому «1» - є найкращим випадком, а «0» - найгіршим.

Але, як відомо, без економічного фактору будь-які визначення не є справедливими. Наведемо коефіцієнт вартості (K_B), що буде визначатись як $K_B = \frac{1}{B}$, де B - вартість системи в умовних одиницях [5], [6], [7].

В загальний добуток додано коефіцієнт масштабування (K_M), де K_M єдиний для усіх систем і визначається для зручності оцінки отриманого результату (50, 100 і т.д.).

Доцільністю систем біометричної ідентифікації та автентифікації вважатимемо адаптивність цих систем до умов їхньої експлуатації, а також їх окремих складових до виконання властивих їм функцій.

Тоді загальний коефіцієнт доцільності використання матиме вигляд:

- Коефіцієнт доцільності використання

$$K_{DB} = K_3 \cdot K_{66} \cdot K_H \cdot K_B \cdot K_M; \quad (1)$$

2. Визначення коефіцієнтів систем

Розглянемо умови експлуатації систем, а також їх окремих складових для виконання властивих їм функцій.

1) Коефіцієнт (K_3), що визначатиме зручність системи. Системи, які вимагають від користувача

^аfobby14@gmail.com

мінімальних дій чи рухів та ідентифікація якими вимагає мінімального часу – матимуть найбільший показник цього параметру і, відповідно, системи, яким для коректної роботи необхідне окреме приміщення і досить тривалий час проведення ідентифікації, та (чи) забезпечення спеціальних умов проведення біометричних вимірів – найменший. В таблиці 1 наведені можливі значення цього коефіцієнту та критеріїв оцінювання.

Таблиця 1. Оцінка зручності системи

Критерій зручності	Необхідність окремого приміщення		Тривалість проведення ідентифікації			Необхідність зміни положення тіла		Універсальність аналізатора біометрії (зручність для людей з різними антропометричними параметрами)		
	K ₁₁		K ₁₂			K ₁₃		K ₁₄		
	Так	Ні	< 2с	2-5с	> 5с	Так	Ні	Макс.	Серед.	Мін.
Значення	0,5	1	1	0,8	0,6	0,8	1	1	0,8	0,6

• Коефіцієнт зручності

$$K_3 = K_{11} \cdot K_{12} \cdot K_{13} \cdot K_{14}; \quad (2)$$

2) Системи використовуються різними людьми, тому виникає необхідність у забезпеченні стерильності поверхонь дотику (для контактних систем ідентифікації) та провітрюванні (вентиляції) приміщень для знімання біометричних показників (таких як голос) для неконтактних систем, оскільки вимагається певна звуко- та шумоізоляція. Для цього використаємо коефіцієнт біологічної безпеки (K_{66}). Системи, які мають найкращу стійкість до передачі різних хвороб – матимуть найбільші значення, а відповідно, системи, які мають найгіршу стійкість – найменші. У таблиці 2 вказані значення коефіцієнту та критеріїв оцінювання.

Таблиця 2. Оцінка біологічної безпеки системи

Критерій біологічної безпеки	Дезінфекція (знезараження) поверхонь чи територій проведення аналізу			Імовірність зараження контактним шляхом			Імовірність зараження повітряно-крапельним шляхом			Забезпечення необхідної гігієни перед проведенням сканування	
	K ₂₁			K ₂₂			K ₂₃			K ₂₄	
	Регул.	Пер.	Відс.	Вис.	Сер.	Низ.	Вис.	Сер.	Низ.	Так	Ні
Значення	0,9	0,6	0,2	0,1	0,5	1	0,25	0,7	0,9	1	0,8

• Коефіцієнт біологічної безпеки

$$K_{66} = K_{21} \cdot K_{22} \cdot K_{23} \cdot K_{24}; \quad (3)$$

3) Всі системи піддаються впливу зовнішніх чинників, чи просто швидше за інших виходять з ладу чи починають гірше працювати внаслідок постійного фізичного контакту, необережності користувачів в ході експлуатації та ін. Тому для дослідження надійності цих систем використовуватимемо коефіцієнт надійності (K_H), складовими параметрами якого будуть критерії, що наведені в таблиці 3. Нижче вказані деякі можливі значення цього коефіцієнту та критеріїв оцінювання (в деяких випадках замість

K_H можливе використання ймовірності безвідмовної роботи P).

Таблиця 3. Оцінка надійності системи

Критерій надійності	Прямий фізичний контакт з пристроєм зчитування		Тривалість роботи до хибного результату перевірки			Вплив зовнішніх факторів на зчитування (вологість, температура, і т.д.)			Ймовірність випадкового пошкодження пристрою зчитування			Мобільність системи	
	K ₃₁		K ₃₂			K ₃₃			K ₃₄			K ₃₅	
	Так	Ні	Дов.	Сер.	Кор.	Вис.	Сер.	Низ.	Вис.	Сер.	Низ.	Так	Ні
Значення	0,8	1	0,9	0,75	0,5	0,4	0,6	0,9	0,3	0,7	0,9	0,5	1

• Коефіцієнт надійності

$$K_H = K_{31} \cdot K_{32} \cdot K_{33} \cdot K_{34} \cdot K_{35};$$

Отже, тепер перевіримо та порахуємо усі коефіцієнти для запропонованих систем, а саме: для відбитків пальців, сканування райдужної оболонки ока, комп'ютерного почерку і аналізу особливостей та характеристик мови.

3. Аналіз результатів оцінки коефіцієнта доцільності

У таблиці 4 наведені результати оцінки K_{DB} при $K_{DB} = 100$, за середньої вартості систем, яка була визначена різними виробниками для пристроїв з однаковим переліком параметрів. Серед них – системи ідентифікації за відбитками пальців, за райдужною оболонкою, за комп'ютерним почерком та за особливостями і характеристиками мовлення.

Таблиця 4. Підсумкові коефіцієнти систем

Система	Відбитки	Райдужна оболонка	Комп'ютерний почерк	Аналіз мови
Зручність	0,6	0,8	0,48	0,3
Безпека	0,216	0,504	0,216	0,144
Надійність	0,151	0,486	0,54	0,21
Загальний	0,108	0,084	0,335	0,064

З отриманих оцінок маємо наступне:

1) Система сканування відбитків пальців виявилась досить зручною у своєму використанні. Низький показник біологічної безпеки зумовлений тим, що для сканерів відбитків пальців вимірювання проводиться без основних гігієнічних вимог (таких як помити руки перед скануванням та ін.) та не проводяться необхідні заходи зі знезараження контактних поверхонь. Тому існує можливість підхопити хворобу внаслідок контакту з зараженою поверхнею. Низька надійність викликана тим, що більшість систем сканування відбитків пальців є мобільними (тобто можуть транспортуватись та переноситись, оскільки мають малогабаритні розміри), тому можуть бути пошкодженими.

2) Система сканування райдужної оболонки ока є зручною і невимовливою до користувача в плані комфорту користування нею. Високий коефіцієнт біологічної безпечності зумовлений тим, що контакт зі спеціальними поверхнями є мінімальним, а приміщення проведення аналізу особи - спеціалізоване.

Але оскільки здебільшого такі системи використовуються у місцях де є потік повітря, то виникає можливість зараження. Система є надійною, хоч і вразлива до багатьох негативних зовнішніх чинників, внаслідок яких можливе погіршення точності сканування.

3) Системи аналізу комп'ютерного почерку. Низьке значення коефіцієнту зручності зумовлене тим, що проведення аналізу даним методом є досить тривалим і для його виконання необхідно змінити положення тіла на комфортне для набору тексту. Окрім того, кожен, хто проходить ідентифікацію таким методом буде користуватись однією клавіатурою. У випадку ж використання «своїх» клавіатур біологічна безпечність методу буде кращою. Система є дуже надійною, оскільки сам пристрій для аналізу не є фізичним, а фізичним є лише пристрій вводу даних.

4) Система аналізу особливостей і характеристик мовлення далеко не найзручніша, та ще і вимагає спеціально облаштованого приміщення. Використання системи не є доцільним у сезон різних вірусних захворювань, оскільки в такому разі висока імовірність підхопити хворобу. Дані системи постійно модернізуються та вдосконалюються, тому їхня надійність залишає бажати кращого.

Отже, як видно з наведених оцінок, системи ідентифікації та автентифікації за клавіатурним почерком виявилися найдоцільнішими.

Аналіз отриманих результатів показує, що якщо не враховувати системи ідентифікації за комп'ютерним почерком (оскільки вони використовуються тільки людьми, які вже присутні на підприємстві), то найкращі результати дає система ідентифікації за відбитками пальців.

Слід зазначити, що для покращення коефіцієнту K_{66} необхідно ускладнювати пристрої за рахунок дезінфекції для кожної окремої особи що проходить перевірку. У свою чергу таке ускладнення призводить до підвищення вартості і, можливо, збільшення часу ідентифікації.

Так, наприклад, для системи ідентифікації за відбитками пальців необхідно застосовувати певні надетонкі плівки, і після кожного дослідження плівка повинна або замінюватись, або переміщуватись щоб відбитки наступної людини, яка буде проходити процес ідентифікації, не потрапили на місце відбитків попередньої.

При ідентифікації людини за райдужною оболонкою ока чи для аналізу мовлення необхідне знищення (чи нейтралізація) можливих вірусів та хвороб, що можуть потрапити в зону проведення ідентифікації. Треба застосовувати пристрої-знезаражувачі або розпилювати спеціальні аерозолі та провітрювати приміщення.

Таким чином, для остаточного обґрунтування вибору потрібне дослідження з біологічної безпеки та зручності для кожного окремого випадку з урахуванням їх особливостей.

4. Висновки

У цій статті був запропонований метод обґрунтування вибору необхідного засобу для проведення біометричної ідентифікації особи при урахуванні коефіцієнта, в якому є такі складові: зручності, біологічної безпеки, надійності та вартості. Попередньо отримані результати показали, що найкращими є системи сканування відбитків пальців. Розвиток цього методу дозволить у кожному конкретному випадку застосовувати найоптимальніший пристрій ідентифікації.

Перелік використаних джерел

1. PROM. Биометрические считыватели отпечатков пальца. — 2018. — Режим доступа: <https://security-systems.co.ua/>.
2. eyeLOCK. EyeLock HBOX, EyeLock Myris. — 2015. — Режим доступа: <https://www.eyelock.com>.
3. Еременко А. В., Сулавко А. Е. Двухфакторная аутентификация пользователей компьютерных систем на удаленном сервере по клавиатурному почерку. — 2015.
4. Nuance. Public security and safety forensic biometric solutions. — 2019. — Режим доступа: <https://www.nuance.com>.
5. Smartvision. Биометрические контроллеры. — 2019. — Режим доступа: <http://smartvision.ua>.
6. Shop Bezpeka. Биометрические считыватели. — 2019. — Режим доступа: <https://www.bezpeka-shop.com>.
7. PROM. Биометрические системы в Украине. — 2018. — Режим доступа: <https://prom.ua>.